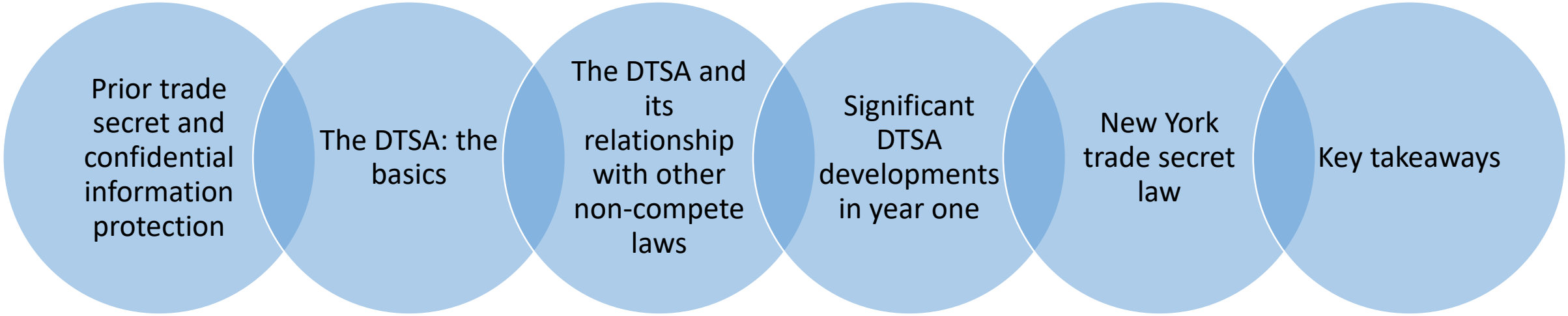
SheppardMullin

Year One: The Defend Trade Secrets Act

How Courts Have Interpreted the DTSA and Reconciled it with the Uniform Trade Secrets Act(s) and Non-Compete Law

Presented by: Kevin M. Cloutier

Overview


Prior trade secret and confidential information protection
The DTSA: the basics
The DTSA and its relationship with other non-compete laws
Significant DTSA developments in year one
New York trade secret law
Key takeaways

Why are we here?

- Trade secret misappropriation has long plagued employers; it is getting worse with technological advances and cyber security issues.
- Employers have a number of weapons in their arsenal in pursuing trade secret misappropriation claims.
- It is important to understand how to best protect trade secret information and how to pursue a claim for the loss or improper use of such information.
- 2016 ushered in a new federal law, the Defend Trade Secrets Act, which has changed the trade secret litigation landscape.

Why are we here?

The DTSA became law in May 2016.

It created a private, federal cause of action for trade secret misappropriation.

The DTSA opened the door to federal jurisdiction for trade secret litigation.

Trade Secret Protection - Overview

Trade secret and non-compete law is vital to any company who values its confidential information.

One of the biggest security risks to the protection of a company's confidential information is its own employees:

- Emailing confidential information to personal email accounts
- Downloading confidential information onto flash drives or other storage devices
- Uploading confidential information to Google Drive or Dropbox

Employee “Theft” Statistics: Misappropriation of Confidential Information

Research firm *Ponemon Institute* conducted survey of 3000+ individuals in six (6) industrialized countries and found:

- More than 50% admitted they had emailed confidential business documents to their personal email address
- More than 40% said they do so at least once per week
- Nearly 40% of employees admitted they use file-sharing applications (such as Google Docs or Dropbox) in the cloud, without employer permission
- More than 50% reported their company does not “strictly enforce” its policies

Why is Employee Misappropriation a Problem?

Technological advances make it easy

- Internet and the cloud (Google Drive, Dropbox, etc.)
- Portable file-sharing devices such as thumb drives, memory sticks, flash drives, external hard drives

Globalization of business operations and markets and corresponding employee mobility

- Competition for employees and customers

Increased pressure to find competitive advantage

Corporate espionage and cyber thieves

Why do these laws matter?

Non-compete, confidentiality, or other restrictive covenant agreements are not always enforceable or even enforced with consistency company-wide.

Even if a company does use non-compete or confidentiality agreements, trade secret laws may still be used to protect confidential information.

The DTSA and other trade secret laws give companies ammunition to prevent misappropriation of trade secret information.

Trade Secrets Landscape Pre-DTSA

The Uniform Trade Secrets Act ("UTSA") provides statutory protection to trade secrets.

48 states and 2 US territories (the U.S. Virgin Islands and District of Columbia) have adopted the UTSA, with some variations.

- Massachusetts and New York protect trade secrets under unique state statutes or common law.

UTSA – Key Definitions

Under the UTSA, a trade secret is information that derives independent economic value and is the subject of reasonable efforts to maintain its secrecy.

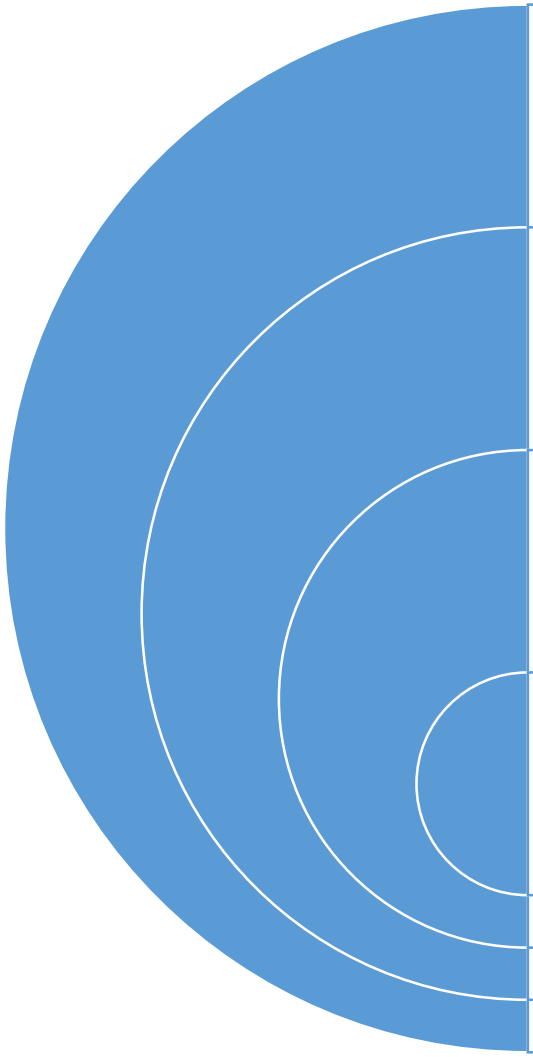
Misappropriation is the disclosure or use of another's trade secret without consent where the acquirer used improper means to acquire the trade secret, or acquired the trade secret from someone who used improper means to get it.

UTSA – Efforts to Maintain Secrecy

Courts emphasize the importance of proactive measures to maintain secrecy of information. Some key examples include:

- Confidentiality and non-disclosure agreements
- Security systems, locked interiors
- Restricted computer access (select user groups, limited authorization, unique credentials, restricted databases)
- Legends on documents: “Confidential” or “Trade Secret”
- Compartmentalize information to those who “need to know”

Computer Fraud and Abuse Act



This federal statute may be used to protect employer's confidential information in conjunction with trade secret laws.

The CFAA imposes liability where someone "intentionally" accesses a computer without authorization or exceeds authorized access, and there obtains . . . Information from any protected computer if the conduct involved an interstate or foreign communication.

The CFAA's original intent was aimed at criminal hacking of computers.

Some jurisdictions expand the CFAA to cover employee trade secret misappropriation.

Computer Fraud and Abuse Act

The CFAA's application to private employers and employee misconduct varies widely across the courts:

Is a true "hacking" required?

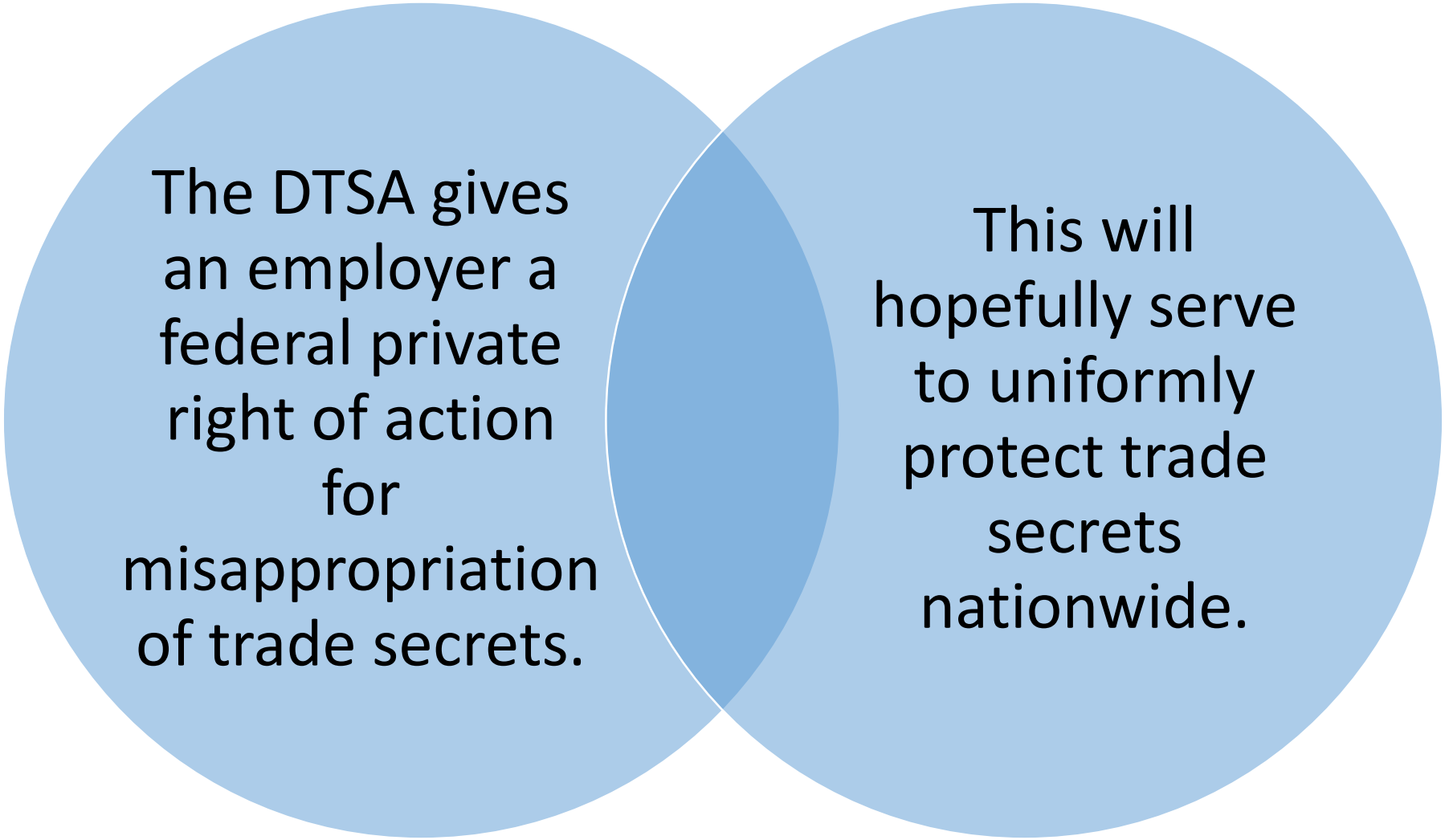
Or, is merely exceeding "authorized access" enough?

The Defend Trade Secrets Act

Highlights:

- Will help to create uniformity in this area of the law and in protecting trade secrets
- Allows for greater remedies such as attorneys' fees, exemplary damages, and a seizure provision
- Does not preempt state trade secret law
- Protects employee whistleblowing activity

Defend Trade Secrets Act – Federal Jurisdiction



Defend Trade Secrets Act – Definition of Trade Secret

The definition of a trade secret is essentially the same as under the UTSA.

The term "trade secret" encompasses a wide array of types of information, and requires:

- The owner thereof has taken **reasonable measures** to keep such information secret; and
- The information derives **independent economic value**, actual or potential, from **not being generally known** to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information.

Defend Trade Secrets Act – Definition of Misappropriation

Misappropriation means either the acquisition of a trade secret by a person who knows or has reason to the know that the trade secret was acquired by improper means, OR

Disclosure of use of a trade secret without consent by a person who:

- Used **improper means** to acquire knowledge of the trade secret
- At the time of disclosure or use, **knew or had reason to know that the knowledge of the trade secret was acquired through improper means** or in violation of a duty to maintain the secrecy of the trade secret; or
- Before a material change of the position of the person, knew or had reason to know that the trade secret was a trade secret and knowledge had been acquired by accident or mistake.

Defend Trade Secrets Act – No Inevitable Disclosure

The DTSA will not permit an injunction restricting an employee from working for a competitor solely based on the inevitable threat of disclosure of trade secrets.

However, the DTSA does not preempt state laws regarding "threatened" trade secret misappropriation.

In jurisdictions where the inevitable disclosure doctrine is an option in trade secret actions, state law remains an important tool alongside the DTSA.

Defend Trade Secrets Act – Seizure Provision

The DTSA has an “ex parte” seizure provision, which allows a plaintiff to ask a court to order law enforcement to physically seize a defendant’s property if necessary to stop dissemination of trade secret.

Courts will only grant this relief under “extraordinary circumstances,” which is very rare.

There is no analogous procedure available under the UTSA.

The Defend Trade Secrets Act - Whistleblowers

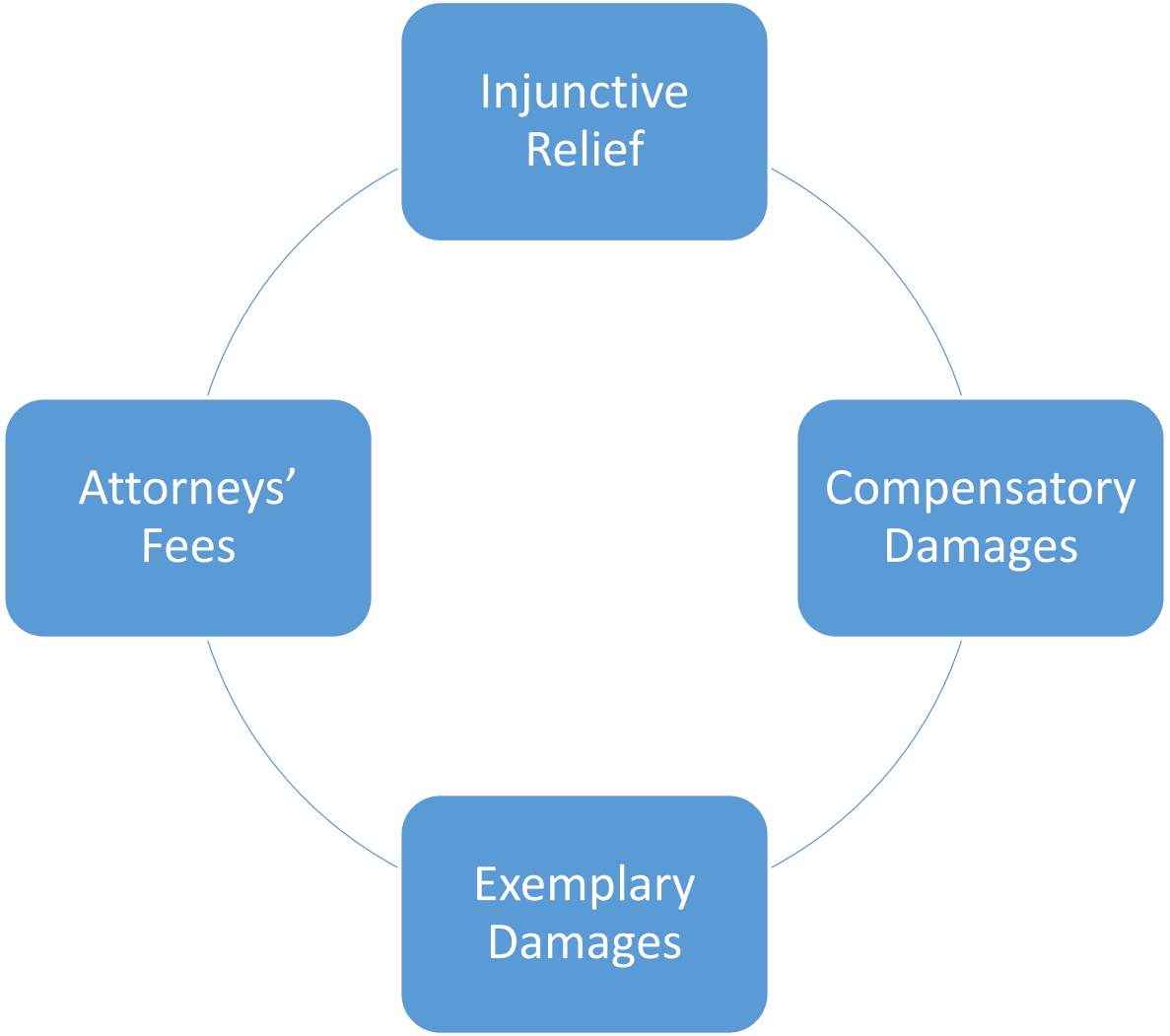
The DTSA expressly protects employee whistleblowing activity.

An employer is prohibited from recovering attorneys' fees and exemplary damages under the DTSA unless the employer has provided notice of immunity from criminal and civil prosecution for disclosure of trade secrets in the course of certain whistleblower activity.

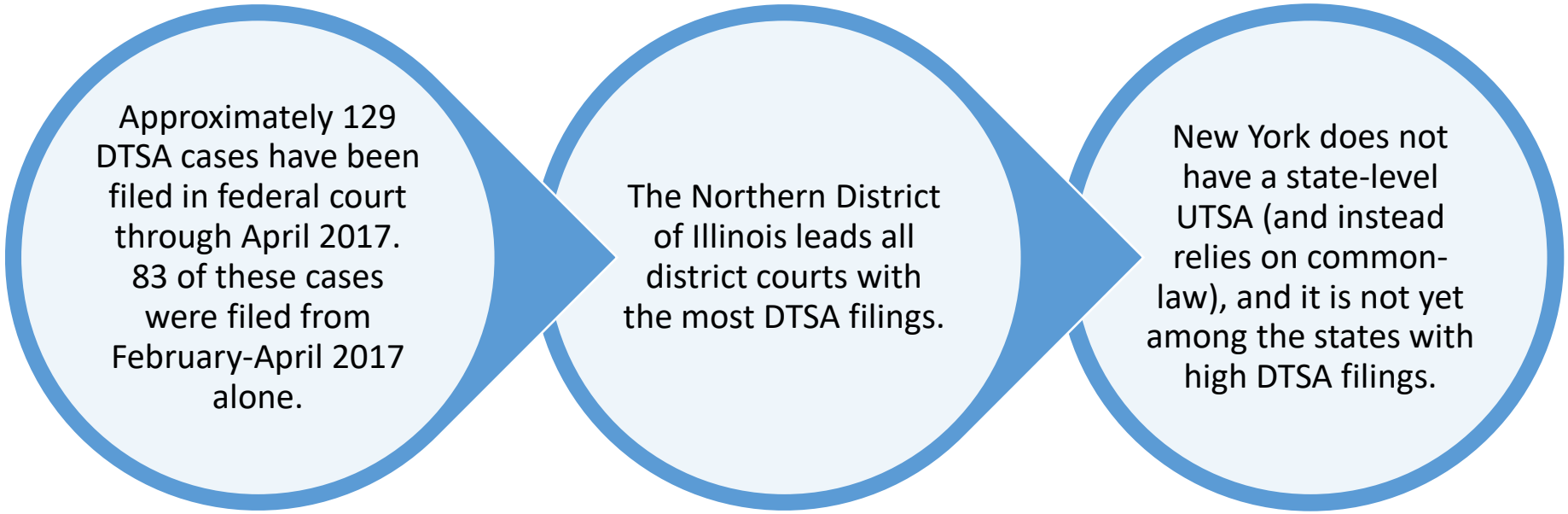
This notice must be provided in writing to the employee in an agreement that governs the use of trade secret or confidential information.

2017 will hopefully bring more clarity and guidance to the provisions of the DTSA, including employee notice and the seizure provision.

Defend Trade Secrets Act - Remedies



Taking a Closer Look at DTSA Cases



Taking a Closer Look at the Seizure Provision

Despite a noticeable uptick in DTSA cases, the seizure provision remains truly an “extraordinary” remedy and is not easily granted.

Critics of the DTSA cautioned against the seizure provision, but courts have been exceedingly cautious in granting seizure applications.

Many courts find that seizure is not “necessary”, and instead issue a TRO covering use and dissemination of such information.

Taking a Closer Look at the Seizure Provision

One of the very few cases granting an application for ex parte seizure came out of the S.D.N.Y.: *Mission Capital Advisors, LLC v. Romaka.*

- Initially, the court denied the seizure application and instead issued a TRO.
- The defendant evaded service of the TRO on 5 separate occasions and failed to appear for the show cause hearing.
- Because the court found it clear that a seizure action was “necessary” because the defendant would evade, avoid or otherwise not comply with the TRO, it ordered seizure of the trade secrets.

A Year Later – The DTSA's Impact

Plaintiffs are pursuing more DTSA cases in federal court. Resolution of these cases will bring more clarity to the limitations and opportunities for companies under the law.

It remains to be seen whether federal court is truly a better venue for trade secrets claims.

The move toward uniformity is also in question as some judges interpret the DTSA alongside UTSA provisions, while others ignore the UTSA and interpret the DTSA anew.

Key Takeaways

Review and update your employee policies and agreements, including confidentiality policies and non-disclosure agreements.

Update your policies to account not only for changes in the law but also for changes in technology.

For example, implement a policy prohibiting employees from using Google Drive or Dropbox to store confidential company information.

Arrange for company training on maintaining confidentiality.

Key Takeaways

Don’t forget the weapons at your disposal if faced with employee trade secret misappropriation:

- The Defend Trade Secrets Act
- Uniform Trade Secrets Act
- Other similar state laws
- The Computer Fraud and Abuse Act
- Actions for breach of contract

Thank You!

Questions?

SheppardMullin